Guida alla
STEGANOGRAFIA D'ASSALTO
a cura di Andrea Pignataro
MZP
254
00 00
Ctrl+W
ÿþ
C:\>copy /b
< >
FF FE
.odt

Guida alla Steganografia d'assalto **a cura di Andrea Pignataro**

Indice

Introduzione

Il termine steganografia è composto dalle parole greche stèganos (nascosto) e gràfein (scrittura) e individua una tecnica risalente all'antica Grecia che si prefigge di nascondere dati sensibili all'interno di altri innocui, rendendoli così inaccessibili a chi non conosce il metodo chiave per accedervi.
Non bisogna confondere la steganografia con la crittografia perchè la steganografia si pone come obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli, mentre per la crittografia è non rendere accessibili i dati nascosti a chi non conosce la chiave.
In parole povere con la crittografia noi ci rendiamo conto dell'esistenza di un file protetto, mentre con la steganografia è l'esistenza stessa del file ad essere nascosta (è quindi più sicura perchè pone i file al riparo da occhi indiscreti e di conseguenza da potenziali attacchi!).

Questa guida è stata creata per illustrare le principali tecniche di steganografia d'assalto, ovvero la steganografia che è possibile applicare su ogni computer (con sistema operativo Windows) senza la necessità di disporre di programmi particolari ma solo di quelli già integrati in Windows oppure di quelli che in media sono già installati sul 90% dei computer.
Questo tipo di steganografia (d'assalto) è nata perchè da sempre quando abbiamo bisogno di sicurezza, ma soprattutto di privacy, per i nostri file ricorriamo a software steganografici che, pur essendo potentissimi e tecnologicamente molto avanzati, necessitano di essere installati sul computer sul quale si vuole aprire il file da loro trattato. E se siamo in ufficio e non abbiamo i permessi d'installazione, oppure non vogliamo installare nulla per non lasciare tracce? O se stiamo utilizzando un computer senza connessione internet e non abbiamo supporti di memoria con su il software steganografico?
A queste domande alcune software house hanno cercato di rispondere creando software "stand-alone", ovvero che non hanno bisogno d'installazione...ma rimane il problema di averlo sempre a disposizione...certo esistono anche gli archivi autoestraenti che richiedono la password...ma per crearli dove il software manca?...e poi sono anche poco sicuri perchè, applicando solo un algoritmo crittografico, si può facilmente scaricare uno dei numerosi programmi "password brute-forcer" (ovvero che ricavano la password dell'archivio provando tutte le possibili combinazioni di caratteri) garantendosi la sprotezione dell'archivio crittografato.
Allora cosa fare?...USARE QUESTA GUIDA!
I metodi descritti in questa guida non richiedono software particolari o non si basano su programmi espressamente steganografici...saremo noi a costruirci la Nostra steganografia!...sarà come seguire un manuale del "fai da te" che permette di costruirvi costosi strumenti prendendo i pezzi da materiale di scarto!

1° metodo: Nascondere un file sensibile in uno innocuo (es. nascondere un file di testo contenente la lista delle vostre password in un file immagine).

Elementi necessari:
per creare il file finale serve:
-il Prompt dei comandi di Windows (cmd.exe; contenuto in ogni versione di Windows, è richiamabile attraverso la funzione “Esegui...” dello Start menu, comunque consiglio di crearsene una copia nella cartella di lavoro per poter eseguire più facilmente le operazioni sui file)
per estrarre il file sensibile o visualizzarlo serve:
-un qualunque editor esadecimale (io consiglio ICY Hexplorer perchè è gratuito ed il migliore nel suo genere...oppure se non volete installare nulla usate hexedit.exe)

Procedimento:
- Avviare il Prompt dei comandi : cmd.exe
- Posizionarsi nella cartella dove sono presenti i file da elaborare (non necessario se il file cmd.exe si trova già nella stessa cartella)
- Digitare (spazi inclusi):
copy /b [file_innocuo] + [file_sensibile] [file_finale]
(dove [file_innocuo] è il nome completo di estensione del file innocuo; [file_sensibile] è il nome completo di estensione del file sensibile; [file_finale] è il nome completo di estensione del file finale)
Esempio:
copy /b fotovacanza.jpg + lemiepassword.txt lamiafotodisicurezza.jpg
- Premere Invio

Quello che otterremo sarà un file che se eseguito funzionerà normalmente (che sia un programma .exe , un immagine .jpg o .bmp , o altro) ma che se aperto con un editor esadecimale potrà:
1.Essere utilizzato per visualizzare il testo di un file .txt nascosto all'interno del file (che si troverà alla fine del file finale visibile per mezzo della colonna laterale dell'editor)
2.Essere tagliato eliminando la parte del file innocuo per ottenere solo la parte esadecimale del file sensibile per poi salvarlo
ATTENZIONE: è necessario ricordarsi perlomeno l'estensione del file sensibile es. ".exe" o altro; ed eliminare il codice esadecimale iniziale solo fino all'header del file sensibile...per sicurezza, prima di elaborare i dati, aprite con l'editor esadecimale il file sensibile e annotatevi l'header...cioè i primi caratteri esadecimali del file, ecco alcuni di quelli più noti:

	estensione		header		header in formato testo
File immagine:	.bmp	=>	42 4D 36	=>	BM6
	.jpg	=>	FF D8 FF	=>	ÿØÿà
	.png	=>	89 50 4E 47	=>	‰PNG
File eseguibile:	.exe	=>	4D 5A 50	=>	MZP
File archivio compresso:	.rar	=>	52 61 72	=>	Rar
	.zip	=>	50 4B 03	=>	PK#

ATTENZIONE:Per preservare l'utilità del file finale, sia esso un immagine o a qualunque altro tipo di file, non lo si deve assolutamente modificare in alcun modo e, logicamente, neanche cancellare.

Suggerimento:Con questo metodo (a patto che non si usino file .txt o altri basati su testo come .html ecc.) al termine di un unione, per esempio di un file .exe e di un file .jpg, è sufficiente cambiare l'estensione del file finale in .jpg o in .exe per accedere al file sensibile o a quello innocuo.

Ammetto che il 1° metodo è un po' difficoltoso, anche se utilizzandolo ci si prende la mano. Comunque non è il mio preferito perchè non su tutti i PC è presente un editor esadecimale.
Il prossimo metodo che illustrerò invece è quello che preferisco maggiormente perchè:
1.Permette di comprimere i file da includere nel file innocuo (così la dimensione elevata dei file più semplici - come i .jpg – non potrà più insospettire);
2.Possibilità di applicare password agli archivi che contengono i file sensibili;
3.L'utilizzo è simile ad una cartella dove possiamo riporre numerosi file sensibili con una sola azione;
4.Anche i file di testo non sono direttamente accessibili (e quindi non sono leggibili neanche con un editor esadecimale)

...e allora eccolo!

2° metodo: Nascondere file sensibili archiviati nel formato .rar in un file innocuo

Sostanzialmente il procedimento di unione dei file è identico a quello del primo metodo ma con una sola variante: il file sensibile è un archivio .rar ,ovvero il reale file sensibile deve essere precedentemente archiviato in .rar con un programma come WinRar e quindi potete applicare anche una password all'archivio creando così un archivio protetto.

Elementi necessari:
per creare il file finale serve:
-il Prompt dei comandi di Windows (valgono le stesse raccomandazioni del primo metodo);
-il software di compressione WinRar
per estrarre o gestire i file sensibili serve:
-il software di compressione WinRar

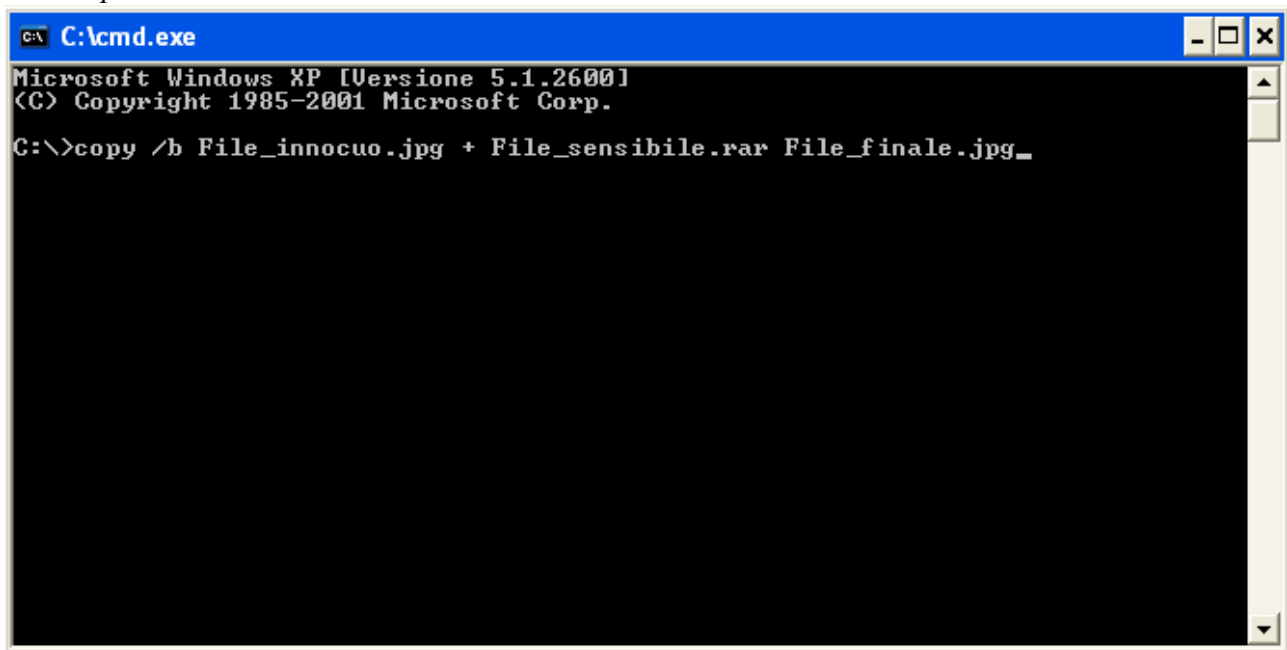
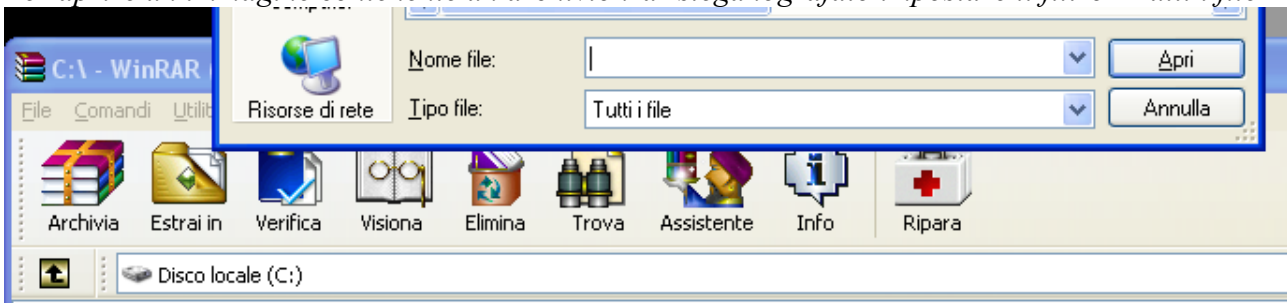
Questa volta consiglio di utilizzare un immagine come file innocuo poiché sono gestiti con più facilità da WinRar che cercherà di interpretarlo come archivio compresso.

Per la creazione del file .rar vi consiglio di seguire questi passi preliminari:
1.Create una cartella con un nome a vostra scelta e inseritevi i file sensibili da nascondere;
2.Se non lo avete già fatto, installate WinRar;
3.Ora fate clic con il tasto destro del mouse sulla cartella contenente i vostri file sensibili e scegliete dal menu: Aggiungi all'archivio “NOME_DELLA_CARTELLA.rar” (dove al posto di NOME_DELLA_CARTELLA ci sarà il nome della cartella contenente i file sensibili)
4.Durante la compressione della cartella in archivio .rar potete cliccare sul pulsante “Opzioni...” per impostare il livello di compressione, se invece volete applicare una password all'archivio dovete scegliere “Aggiungi ad un archivio...” dal menu del punto 3 e dal tab “Avanzati” della finestra che comparirà cliccare il pulsante parola chiave, digitare la password, premere Ok e ancora Ok nella finestra principale.
5.Ora avete ottenuto il file .rar da utilizzare.

Procedimento:
- Avviare il Prompt dei comandi : cmd.exe
- Posizionarsi nella cartella dove sono presenti i file da elaborare (non necessario se il file cmd.exe si trova già nella stessa cartella)
- Digitare (spazi inclusi): copy /b [file_innocuo] + [file_sensibile.rar] [file_finale]
(dove [file_innocuo] è il nome completo di estensione del file innocuo; [file_sensibile.rar] è il nome completo di estensione del file .rar; [file_finale] è il nome completo di estensione del file finale)
Esempio: copy /b fotovacanza.jpg + lemiepassword.rar lamiafotodisicurezza.jpg
- Premere Invio.

Ora quello che otteniamo è un file immagine che se aperto con WinRar mostrerà i file in esso contenuti che si potranno estrarre o aggiungerne altri (per aprire il file immagine bisogna impostare il filtro “Tutti i file” nella finestra di WinRar che ci chiederà quale file aprire).

Ho scelto il formato .rar perchè in confronto agli altri formati di compressione (come .zip, .ace ecc...) offre:
-Il più alto rapporto di compressione presente;
-Nessun limite della grandezza dei file da comprimere;
-Cerca di interpretare qualunque formato di file come un archivio compresso in .rar andando alla ricerca dell'header;
-Possibilità di commentare il file compresso e tante altre configurazioni che ottimizzano il processo di compressione.
ATTENZIONE:Per preservare l'utilità del file finale, non lo si deve assolutamente modificare in alcun modo e, logicamente, neanche cancellare.

Il Prompt dei comandi di Windows

Per aprire un immagine contenente un archivio .rar steganografato impostare il filtro “Tutti i file”

3° metodo: Steganografia asiatica

Questo metodo si discosta molto dai primi due.
Esso si basa su un bug del famoso “Blocco note” di Windows: quando noi vogliamo aprire un file e vogliamo osservarne la struttura in forma pura lo apriamo con il “Blocco note”...lo facciamo per i file .html , .php , .doc ed altri formati...perchè lo facciamo? Perchè “erroneamente” pensiamo che il “Blocco note” non elabora...non interpreta.
...e invece non è così!!!
Il “Blocco note” interpreta!...o almeno cerca di farlo...e quando fallisce? ...ecco che entra in azione il 3° metodo!
Prima di tutto vorrei spiegare perchè l'ho chiamato “steganografia asiatica”: questo metodo fa fallire volontariamente l'interpretazione euristica del “Blocco note” e trasforma tutti i caratteri in caratteri cinesi...quindi il testo risultante se venisse tradotto (o letto da un cinese) non sarebbe altro che un insieme strampalato di parole senza alcun nesso tra di loro che in verità nascondono il testo sensibile che vogliamo proteggere. A prima vista può sembrare che tale metodo non sia steganografico ma che si limiti solo ad alterare il testo ... invece è un metodo steganografico perchè altera il testo sensibile in altro testo con un significato totalmente innocuo che nasconde tra le righe il vero testo sensibile (anche se noi il cinese non lo sappiamo leggere ci sono software di traduzione appositi...provare per credere!).
Anche se il file finale viene aperto con il WordPad o con qualunque altro software di videoscrittura compariranno i caratteri cinesi a sostituire quelli normali, ma è importante che il file iniziale sia stato creato con il “Blocco note”.
Se il file finale viene aperto con il “Blocco note” di Windows Xp verranno visualizzati dei quadrati bianchi al posto dei caratteri cinesi, ma in entrambi i casi un osservatore esterno non riuscirà in alcun modo a comprendere il testo sensibile.

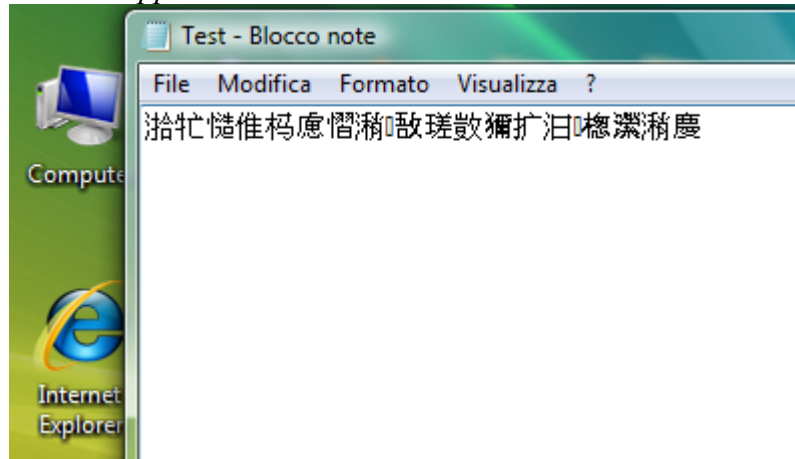
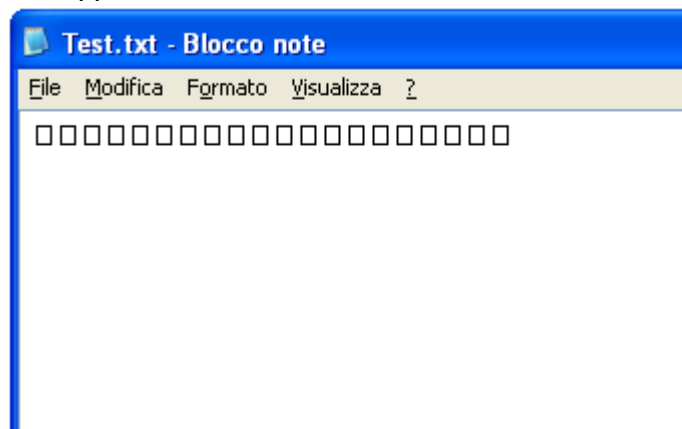
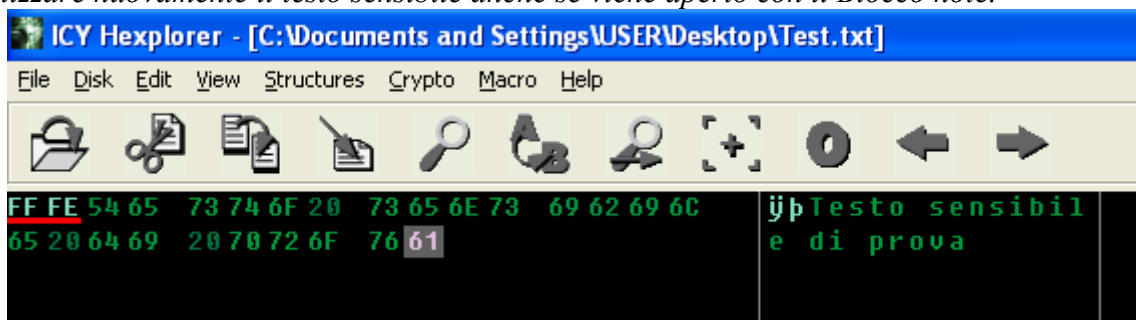
Elementi necessari:
per creare il file finale serve:
-il “Blocco note” di Windows
per visualizzare il file sensibile serve:
-il “Blocco note” di Windows
-un qualunque editor esadecimale

Procedimento:
-Aprite il “Blocco note”;
-Tenere premuto il tasto Alt sulla tastiera e premere contemporaneamente la sequenza di numeri 0255 sul tastierino numerico;
-Rilasciare il tasto Alt e ripetere l'operazione precedente solo che questa volta la sequenza di numeri sarà 0254;
-Ora potete andare subito a capo oppure continuare a scrivere il vostro testo sensibile (o copiate e incollateci uno già preparato) di seguito ai due caratteri che si sono creati (ÿþ);
-Salvate il file .txt con un nome qualsiasi;

Ora se provate a riaprire il file che avete creato il risultato sarà una pagina piena di caratteri cinesi (oppure se state usando il “Blocco note” di Windows Xp vedrete solo dei quadrati bianchi).

Per recuperare il testo sensibile seguite questi semplici passi:
-Aprite il file finale con un editor esadecimale;
-Modificate i primi due valori esadecimali “FF FE” in “00 00”;
-Salvate;
-Ora aprite il file con qualunque programma di videoscrittura (anche lo stesso “Blocco note”) per visualizzare il testo sensibile.

Se volete riapplicare questo metodo steganografico immediatamente dopo aver visualizzato il testo sensibile eseguite questi passaggi:
-Aprite il file con il “Blocco note”;
-Cancellate i due spazi all'inizio del testo;
-Posizionare il cursore di scrittura all'inizio del testo;
-Tenere premuto il tasto Alt sulla tastiera e premere contemporaneamente la sequenza di numeri 0255 sul tastierino numerico, rilasciate il tasto Alt e ripetete l'operazione solo che questa volta la sequenza di numeri sarà 0254;
-Salvate (non “Salva con nome” ma “Salva”).

Il risultato dell'applicazione del 3° metodo sul Blocco note di Windows Vista

Il risultato dell'applicazione del 3° metodo sul Blocco note di Windows Xp

I due valori esadecimali sottolineati in rosso “FF FE” devono essere cambiati in “00 00” per visualizzare nuovamente il testo sensibile anche se viene aperto con il Blocco note.

4° metodo: Inchiostro simpatico

Questo 4° metodo può essere tranquillamente definito come la versione digitalizzata dell'inchiostro simpatico (quello con lo stecchino, il succo di limone e la candela) che quasi tutti da bambini abbiamo provato a fare. Quello che ora andremo ad esaminare si basa principalmente su una questione cromatica dove i colori sono steganografati: ogni colore, R (rosso), G (verde) e B (blu), nell'ambito dei computer posseggono 256 variazioni di tonalità, ovvero da 0 a 255...noi sfrutteremo le variazioni di 1, precisamente quella che va da 255 a 254...la differenza tra questi due valori è talmente minima da essere perfettamente "nascosta" ai nostri occhi ed anche ai nostri monitor...ma non lo è ai nostri computer che non lavorano su un piano visivo ma bensì su uno numerico. Se applichiamo un valore tonale di 255 a tutti e tre i colori (R-G-B) otteniamo il colore bianco...se invece applichiamo un valore tonale di 254 otteniamo...sempre bianco!!! ...almeno visivamente. Infatti è proprio su questo difetto ottico (assolutamente naturale) che lavoreremo: per una volta apprezzeremo la differenza che c'è tra un essere umano e un computer, perchè imponendo al computer di applicare un filtro che lasci invariato il bianco, e quindi tutto ciò che ha valore tonale di 255 su ogni piano cromatico R-G-B, e che trasformi tutto ciò che non lo è in nero (e il valore 254 su ogni piano cromatico R-G-B non lo è!) otterremo una steganografia letteralmente "invisibile"!
Non preoccupatevi...anche se questo metodo sembra complesso vedrete che applicarlo è più facile di quanto si possa pensare!

Elementi necessari:
per creare il file finale serve:
-il "Paint" di Windows presente in ogni versione di Windows
per visualizzare il file sensibile serve:
-il "Paint" di Windows presente in ogni versione di Windows

Procedimento:
-Aprire il "Paint" di Windows;
-Estendere l'area di disegno quanto lo si vuole;
-Dal menu degli strumenti a sinistra scegliere la funzione testo;
-Tenere cliccato e trascinare il cursore per estendere l'area di testo della grandezza che si vuole;
-Scrivere i dati sensibili o incollarli (devono essere stati precedentemente copiati) tramite la combinazione di tasti Ctrl+V;
-Selezionare il testo digitato trascinando il cursore sul testo fino ad evidenziarlo completamente;
-Cliccare dal menu in alto la voce "Colori" e successivamente dal menu a tendina "Modifica colori...";
-Ora nella finestra "Modifica colori" cliccare sul pulsate "Definisci colori personalizzati>>";
-Adesso dovete inserire in ogni piccolo riquadro bianco alla destra delle scritte Rosso, Verde e Blu il valore 254;
-Premete il pulsante "Ok"
-Ora cliccate il primo quadrato bianco della barra dei colori che sitrova a sinistra partendo dall'alto;
-Salvate l'immagine come Bitmap a 24 bit (.bmp) con un nome a vostra scelta.

Ora se provate ad aprire l'immagine con un qualunque programma di visualizzazione (o anche solo a stamparla) vedrete solamente un immagine completamente bianca...e in effetti visivamente lo è ...ma non numericamente!
Quindi ora vediamo come riuscire a visualizzare il testo sensibile che avevamo scritto nell'immagine...no, non vi servono le candele...ma solamente di nuovo il "Paint"!

-Aprite l'immagine finale con il "Paint" di Windows;
-Cliccate sulla voce del menu in alto "Immagine" e successivamente dal menu a tendina "Attributi..." ;

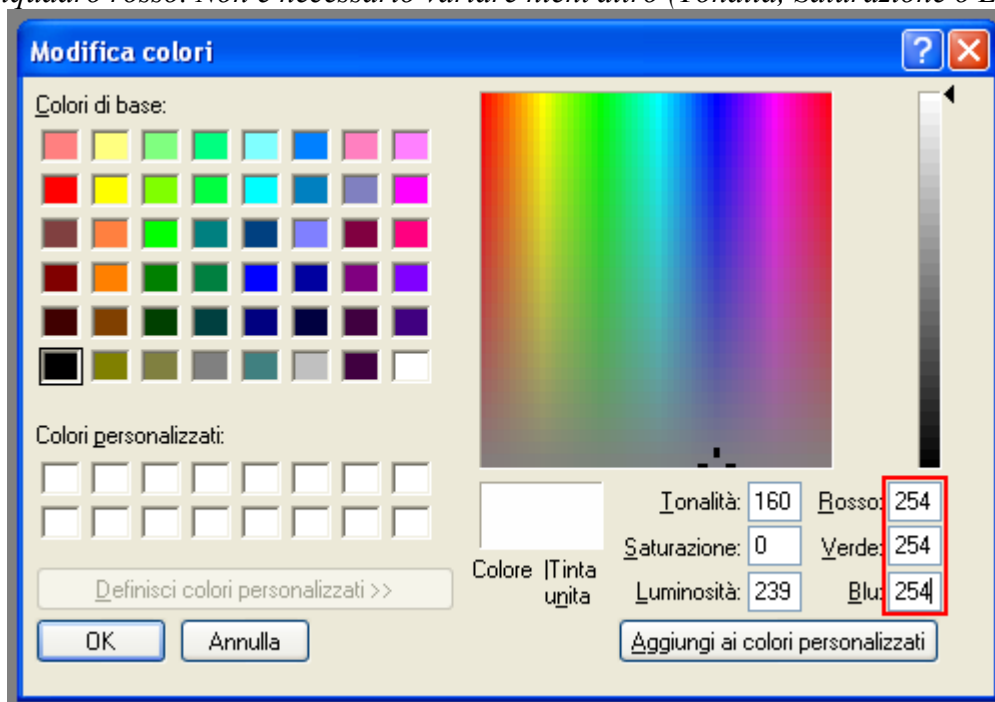
-Ora nel riquadro “Colori” cambiate il segno di selezione da “Colori” a “Bianco e nero”;
-Cliccate sul pulsante “Ok”;
-Confermate la finestra che vi avviserà che ci saranno delle perdite di informazioni sul colore cliccando sul pulsante “Sì”;
-Ed ecco che apparirà il vostro testo (proprio come il succo di limone e la candela).

Ora potete risalvare l'immagine in qualunque formato “Paint” vi permette di farlo e così visualizzarla con il vostro programma di visualizzazione immagini preferito!

Come avrete sicuramente notato, non ho menzionato affatto il disegno libero...non l'ho fatto semplicemente perchè se disegnate con il colore nero (o con qualunque altro colore di facile visualizzazione) in “Paint”, dopo non potete più cambiare il colore nel Bianco 254 (R:254-G:254-B:254) o almeno potete utilizzare la funzione di riempimento ... ma diventa estenuante se il disegno diventa un minimo complesso, mentre come avete visto con la scrittura è possibile farlo “al volo”.
Ma non vi sarete arresi per così poco? Non esiste solo Paint!
Infatti se utilizzate un altro programma di grafica tipo Photoshop o The Gimp potete cambiare il colore di un intero disegno, anche molto complesso, dopo averlo creato...basta seguire questi semplici passi che più o meno sono uguali per tutti i programmi grafici:

1.Aprite il programma grafico;
2.Create una nuova immagine completamente nera;
3.Ora aggiungete un livello trasparente sovrapposto allo sfondo nero creato;
4.Disegnate su questo livello trasparente utilizzando il colore Bianco 254 (R:254-G:254-B:254);
5.Ora selezionate il livello dello sfondo nero e cambiatene il colore (anche con un semplice riempimento) nel Bianco 255 (R:255-G:255-B:255);
6.Salvate l'immagine come Bitmap a 24 bit (.bmp) con un nome a vostra scelta.

Ora avete una complessa immagine da visualizzare con il “Paint” sfruttando lo stesso procedimento di visualizzazione che è stato usato prima.

Per ottenere il “bianco 254” (il nostro inchiostro simpatico) si devono variare i valori dei colori come nel riquadro rosso. Non è necessario variare nient'altro (Tonalià, Saturazione o Luminosità).

5° metodo: Steganografia .html

Ora affronteremo un tipo di steganografia che nasconde i testi sensibili nei file .html, .php, .htm .... ovvero le pagine web che scarichiamo da Internet o che (se ne abbiamo la capacità) ci creiamo per allestire il nostro sito web.
Il punto di forza di questo metodo (ancora una volta) è l'interpretazione della formattazione dei testi: i file .html (o qualunque altro formato di file delle pagine web) sono sempre associati ai browser Internet che sono installati di norma su tutti i computer del pianeta, qualunque browser sia ...Internet Explorer, Firefox, Opera, Safari... interpreta i file web secondo una formattazione standard stabilita dal W3C (World Wide Web Council), tale formattazione ci permetterà di inserire un testo sensibile all'interno di un qualunque file web a condizione che abbia un contenuto innocuo che sia formattato secondo lo standard del W3C (una qualunque pagine web presente su Internet andrà bene).
Quindi prima di cominciare procuriamoci una pagina web presente su Internet aprendo il nostro browser di fiducia e utilizzando la funzione classica "Salva con nome...".

Elementi necessari:
per creare il file finale serve:
-un file pagina web (.html - .php - .htm ecc.)
-il "Blocco note" di Windows o qualunque altro editor di testo non formattato
per visualizzare il testo sensibile serve:
-il "Blocco note" di Windows o qualunque altro editor di testo non formattato

Procedimento:
-Aprite il file della pagina web con il "Blocco note" di Windows o qualunque altro editor di testo non formattato;
-Posizionate il cursore di scrittura in fondo al testo e per sicurezza premete il tasto Invio in modo di andare a capo assicurandosi di non avere alcun carattere davanti o dietro il cursore di scrittura;
-Digitate il vostro testo sensibile tra questi caratteri: < >
es.:
<Testo sensibile>
...potete sia applicare i due simboli per ogni riga tutte le volte che andate a capo oppure applicare il simbolo < all'inizio, scrivere il vostro testo sensibile, anche andando a capo, e alla fine del testo digitare il simbolo >
es.:
<Testo sensibile
testo sensibile
testo sensibile>
-Salvate il testo con la funzione "Salva" e non "Salva con nome...".

Ora se aprite il file della pagina web con qualunque browser Internet (basterà cliccarci sopra per aprirlo in automatico con il browser Internet installato sul vostro computer) non visualizzerete in alcun modo il testo sensibile ma soltanto la pagina web così come l'avevata scaricata.
Per visualizzare il testo sensibile dovrete semplicemente aprire la pagina web con il "Blocco note" di Windows (o qualunque altro editor di testo non formattato). Se volete visualizzare il testo sensibile anche dopo aver aperto la pagina web con un browser Internet sarà necessario eliminare i simboli < > dal testo sensibile e salvare con "Salva" e non "Salva con nome...".

6° metodo: Steganografia musicale (CD-AUDIO)

Basandoci sul 2° metodo (per motivi di versatilità) ora impareremo a nascondere i nostri file sensibili nei CD-AUDIO che potremo continuare ad ascoltare in qualsiasi lettore CD senza intaccare minimamente la qualità audio con rumori o errori durante la riproduzione...cose che farebbero insospettire immediatamente riguardo al reale contenuto del disco.
Per prima cosa dobbiamo creare un archivio .rar contenente i nostri file sensibili (come spiegato nel 2° metodo).
Ora invece dobbiamo preparare la nostra musica da masterizzare sul CD-AUDIO, per fare ciò è necessario convertire (se non lo sono già) i nostri file musicali nel formato .wav (massimo a 16 bit...non vi preoccupate nel 99% dei casi non c'è bisogno di controllare nulla) ... potete farlo con qualsiasi programma che lo permette ... ma di solito su un computer ne è sempre presente uno (da anni la suite di Nero include un WaveEditor che funziona anche da convertitore).
Una volta che abbiamo a disposizione il file .rar che contiene i nostri file sensibili, i file audio in formato .wav e un cd-rom vuoto da masterizzare siamo pronti ad applicare il seguente metodo steganografico.

Elementi necessari:
per creare il file finale serve:
-il Prompt dei comandi di Windows
-il software di compressione WinRar
-il file .rar contenente i vostri file sensibili
-i file audio in formato .wav
per estrarre i file sensibili serve:
-il software di compressione WinRar

Procedimento:
- Avviare il Prompt dei comandi : cmd.exe
- Posizionarsi nella cartella dove sono presenti i file da elaborare (non necessario se il file cmd.exe si trova già nella stessa cartella)
- Digitare (spazi inclusi): copy /b [file_audio.wav] + [file_sensibile.rar] [file_finale.wav]
(dove [file_audio.wav] è il nome completo di estensione del file audio; [file_sensibile.rar] è il nome completo di estensione del file .rar; [file_finale.wav] è il nome completo di estensione del file finale) Esempio: copy /b musica.wav + lemiepassword.rar lamiamusicadisicurezza.wav
- Premere Invio.

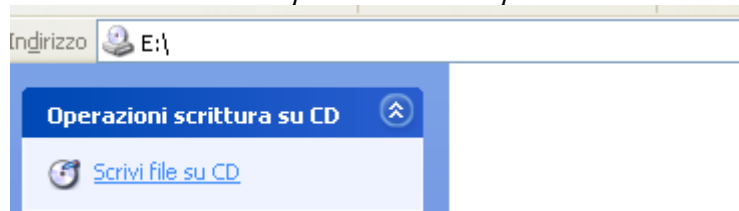
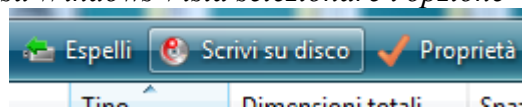
Logicamente quello che otteniamo è un solo file audio .wav, se invece abbiamo più archivi .rar contenenti file sensibili dovremo ripetere la stessa procedura per più file audio .wav.
Poniamo per esempio che abbiamo creato 4 file audio .wav contenenti rispettivamente 4 file .rar sensibili; i file sono canzoni diverse che andremo a masterizzare su un cd-rom con un qualunque programma di masterizzazione ... ma con una sola accortezza: MASTERIZZARE IL CD-ROM COME CD DATI E NON COME CD AUDIO, se utilizziamo Nero per masterizzare scegliamo "Creare cd dati" mentre se usiamo un altro software cerchiamo la funzione di masterizzazione cd dati ... se invece non abbiamo software di masterizzazione ma il nostro sistema operativo è Windows Xp o Windows Vista possiamo masterizzare un cd dati semplicemente inserendo il cd-rom vuoto nel masterizzatore, aprire la finestra di esplorazione del suo contenuto (clic con il tasto destro del mouse sull'icona del masterizzatore e cliccare su Esplora) e dopo averci trascinato dentro i file audio .wav creati cliccare:
-Windows Xp: dal menu a sinistra la voce "Scrivi file su CD"
-Windows Vista: dal menu contestuale in alto "Scrivi su disco"
Ora anche se quello che abbiamo masterizzato è un CD dati non dobbiamo preoccuparci perchè il formato .wav dei file audio viene letto ugualmente da tutti i lettori CD come se fosse un CD Audio

perchè il formato .wav è un formato grezzo...nel senso che non comporta perdita di qualità o compressioni ma contiene l'audio così com'è nella sua forma più pura.
Quindi ora abbiamo ottenuto un CD Audio che comporta alcuni vantaggi:
-facile esportazione dei file audio
-possibilità di dare un nome alle tracce (infatti il nome del file .wav potrà essere il titolo del brano musicale)
-applicabilità steganografica

Per estrarre i file sensibili basterà aprire i file .wav con WinRar che mostrerà i file contenuti nei file .rar steganografati (per aprire i file .wav bisogna impostare il filtro “Tutti i file” nella finestra di WinRar che ci chiederà quale file aprire) oppure se prima copiamo i file audio sul computer possiamo cambiarne l'estensione in .rar per trasformarli in archivi compressi e quindi facilitarne anche l'apertura.
Come avrete notato la tecnica steganografica è identica a quella del 2° metodo con la sola differenza che questa volta abbiamo usato dei file audio .wav come file innocui, quindi consiglio di sfruttare l'opportunità di applicare delle password agli archivi in .rar, prima di steganografarli nei file .wav, in modo da aumentare notevolmente la sicurezza.

ATTENZIONE:Per preservare l'utilità del file finale, non lo si deve assolutamente modificare in alcun modo e, logicamente, neanche cancellare.

Per masterizzare un CD dati con il software Nero selezionare l'opzione “Creare CD dati” *dal menu* “Dati” *di Nero Start Smart.*

Per masterizzare un CD dati su Windows Xp selezionare l'opzione “Scrivi file su CD”.

Per masterizzare un CD dati su Windows Vista selezionare l'opzione “Scrivi su disco”.

7° metodo: Nascondere file sensibili nei file OpenDocument

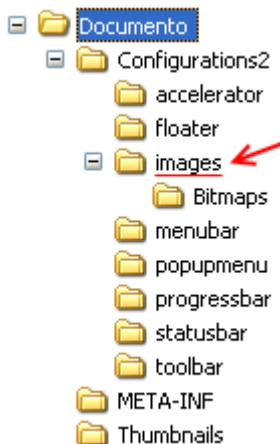
I file OpenDocument sono un alternativa a struttura aperta ai file .doc di Microsoft Office.
Il formato dell'OpenDocument è .odt ed è supportato nativamente in scrittura e in lettura dalla suite OpenOffice della Sun Microsystems e da molti altri software di videoscrittura opensource.
Questo formato particolare ci tornerà utile proprio grazie alla sua struttura aperta...vediamo come!

Elementi necessari:
per creare il file finale serve:
-un file in formato .odt (OpenDocument)
-un programma per gestire i file .zip...WinRAR andrà benissimo
per estrarre i file sensibili serve:
-un programma per gestire i file .zip come WinRAR

Procedimento:
-Cambiare l'estensione del file .odt in .zip
-Aprire il file .zip con WinRAR (o con qualunque altro gestore di file .zip)
-Recarsi nella cartella dentro il file .zip: Configurations2\images\
-Trascinare i file sensibili in questa cartella
-Chiudere WinRAR
-Cambiare l'estensione del file .zip in .odt

Ora il file .odt conterrà i file sensibili e anche se aperto con un editor di testo predisposto per questo formato non visualizzeremo in alcun modo i file sensibili. La cartella “Configurations2\images\” è stata scelta perchè, anche se modificherete il file .odt continuandolo ad usare come documento di testo e a salvarne le modifiche, i file sensibili rimarranno lì dove sono senza subire modifiche o cancellazioni.

Naturalmente per estrarre i file sensibili dal file .odt sarà necessario cambiare l'estensione del file da .odt in .zip e di seguito aprirlo con un programma per gestire i file .zip per estrarne il contenuto ricordandosi che i file sensibili si trovano nella cartella “Configurations2\images\” all'interno della cartella che è nominata come il file .odt (ormai divenuto .zip).

*Questa è la struttura interna standard di un documento .odt. I file da nascondere devono essere inseriti nella cartella “*images*” (sottolineata in rosso e indicata dalla freccia rossa).*

8° metodo: Steganografia ottica

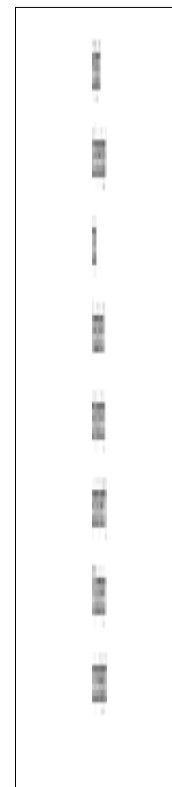
Basandosi su un famoso effetto ottico, questo metodo nasconde un testo sensibile in un'immagine che mostra solo delle incomprensibili linee verticali...in altre parole è come se scriviamo su di un foglio una parola allungandola esageratamente nella direzione verticale, in modo tale da non essere leggibile, per poi inclinare il foglio sull'asse orizzontale e rendere la parola precedentemente scritta perfettamente leggibile.
Noi però non scriveremo sulla carta il nostro testo sensibile ... ma simuleremo l'esperienza utilizzando il "Paint" di Windows e le sue funzioni:
-"Testo" per la videoscrittura;
-"Allunga/Inclina" (o "Ridimensiona/Inclina" se il "Paint" è di Windows Vista) per lo "stretching" delle immagini.
Se avessimo utilizzato la carta, sarebbe bastato inclinare il foglio per leggere il testo ... ma tutto ciò sarebbe stato oltre che insicuro anche limitativo poichè ci sarebbe voluto un foglio di carta lungo una decina di metri solo per scrivere una frase seguendo questa tecnica!
Utilizzando il "Paint" sfrutteremo alcune caratteristiche della sua gestione dello "stretching" ("stiramento") delle immagini. Infatti il "Paint" "stira" verticalmente le immagini in modo graduale: una composizione articolata di punti neri viene trasformata in linee con sfumature grigie; tale metodo di "stretching" incrementa l'incomprensibilità del testo steganografato rendendolo sicuro anche se venisse stampato.
Inoltre poichè utilizziamo il computer è bene sfruttare la possibilità di spingersi ai limiti: "stireremo" il testo di una percentuale che dopo alcuni test ritengo che sia un buon compromesso tra gestione del file finale e sicurezza del metodo steganografico: 1500%
Il "Paint" di Windows purtroppo ci permette di "stretchare" le immagini solo del 500% alla volta, quindi dovremo applicare lo "stretching" del 500% per tre volte.
Per far ritornare l'immagine alla sua dimensione normale (e quindi per rendere nuovamente il testo leggibile) dovremo "comprimerla" verticalmente due volte : prima al 9% e dopo all'8%.

Elementi necessari:
per creare il file finale serve:
-il "Paint" di Windows presente in ogni versione di Windows
per visualizzare il file sensibile serve:
-il "Paint" di Windows presente in ogni versione di Windows

Procedimento:
-Aprire il "Paint" di Windows;
-Estendere l'area di disegno quanto lo si vuole;
-Dal menu degli strumenti a sinistra scegliere la funzione testo;
-Tenere cliccato e trascinare il cursore per estendere l'area di testo della grandezza che si vuole;
-Selezionare dalla barra degli strumenti di testo la dimensione 8 (consigliata ma non necessaria);
-Scrivere i dati sensibili o incollarli (devono essere stati precedentemente copiati) tramite la combinazione di tasti Ctrl+V;
-Selezionare dal menu "Immagine": "Allunga/Inclina" (o "Ridimensiona/Inclina" se il "Paint" è di Windows Vista) o digitare Ctrl+W;
-Digitare 500 nel box "Verticalmente" dell'area "Allunga" (o "Ridimensionamento" se il "Paint" è di Windows Vista);
-Cliccare sul pulsante "OK" e ripetere queste ultime tre azioni altre due volte;
-Salvare l'immagine creata (consiglio il formato JPEG perchè salvando l'immagine in BMP si possono facilmente raggiungere dimensioni spropositate a causa dell'elevata estensione dell'immagine dovuta allo "stretch" applicato).

Per rendere il testo sensibile nuovamente leggibile è necessario aprire l'immagine salvata con il

"Paint" e seguire questi semplici passaggi:
-Selezionare dal menu "Immagine": "Allunga/Inclina" (o "Ridimensiona/Inclina" se il "Paint" è di Windows Vista) o digitare Ctrl+W;
-Digitare 9 nel box "Verticalmente" dell'area "Allunga" (o "Ridimensionamento" se il "Paint" è di Windows Vista);
-Cliccare sul pulsante "OK";
-Selezionare dal menu "Immagine": "Allunga/Inclina" (o "Ridimensiona/Inclina" se il "Paint" è di Windows Vista) o digitare Ctrl+W;
-Digitare 8 nel box "Verticalmente" dell'area "Allunga" (o "Ridimensionamento" se il "Paint" è di Windows Vista);
-Cliccare sul pulsante "OK".

Ora è possibile salvare l'immagine con il testo sensibile rivelato oppure, dopo averla visualizzata, chiudere il "Paint" senza salvare le modifiche apportate lasciando così intatto il file steganografico.

In conclusione voglio lasciarvi un esercizio da svolgere, ovvero dovete trovare un messaggio che ho steganografato in questa guida con un metodo non descritto...ma facilmente desumibile se avete letto attentamente questa guida...

Per maggiori informazioni, domande o suggerimenti scrivete al mio indirizzo e-mail: *andreasoftware1990@libero.it*

Buona caccia al messaggio!

"Il modo migliore per proteggere una cosa è nasconderla tra molte altre cose simili ad essa, così solo chi saprà esattamente dove guardare troverà la cosa giusta."

- Andrea Pignataro - 2008